STATE PRIVACY OFFICER

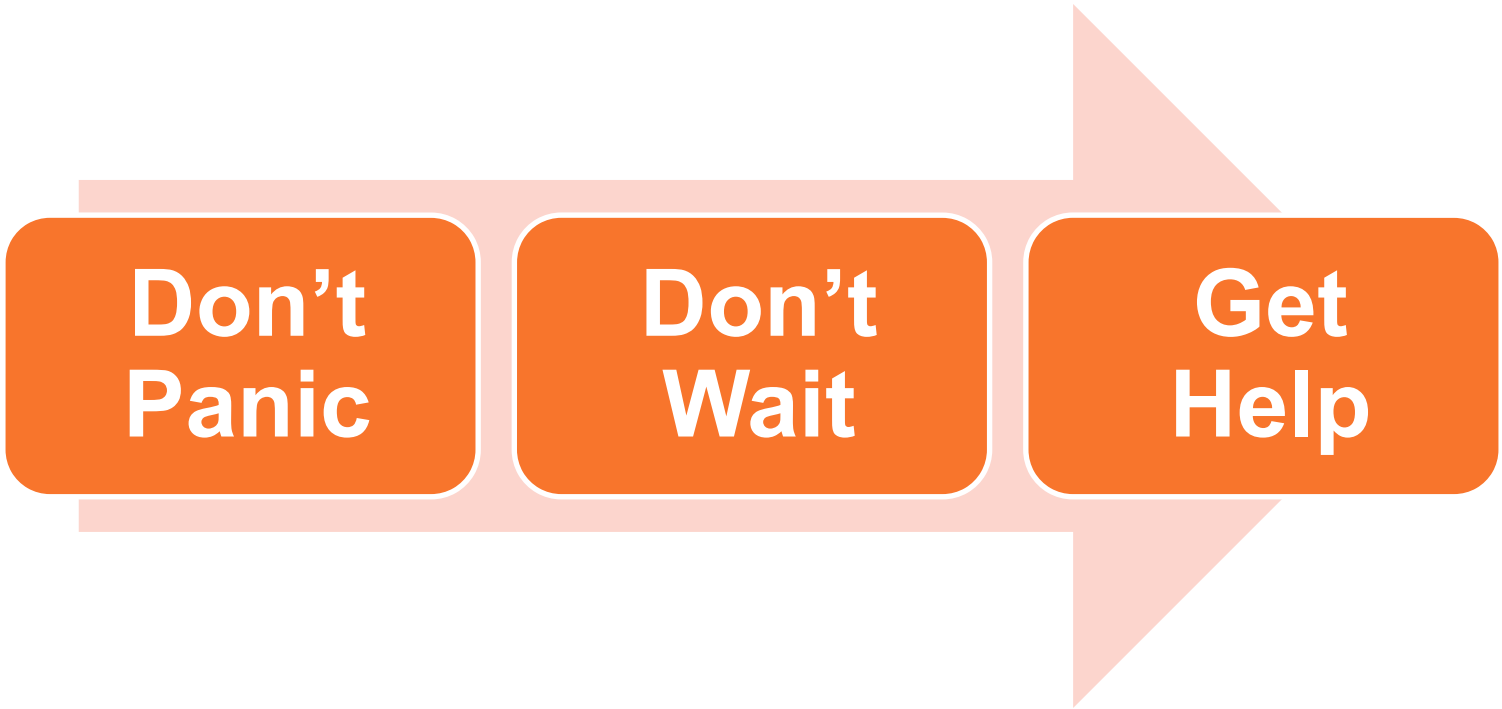
Dr. Whitney Phillips

wphillips@Utah.gov

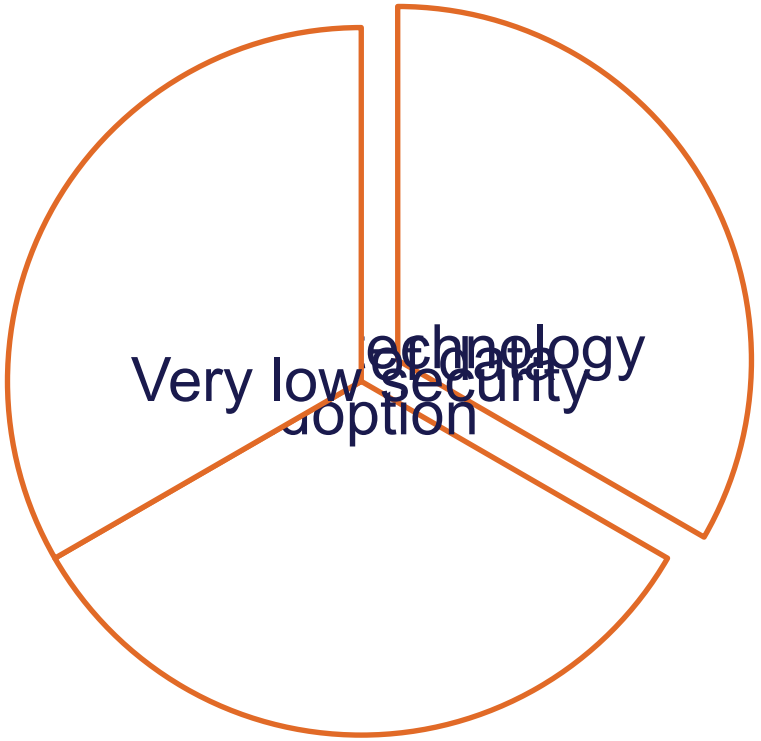
April 2022

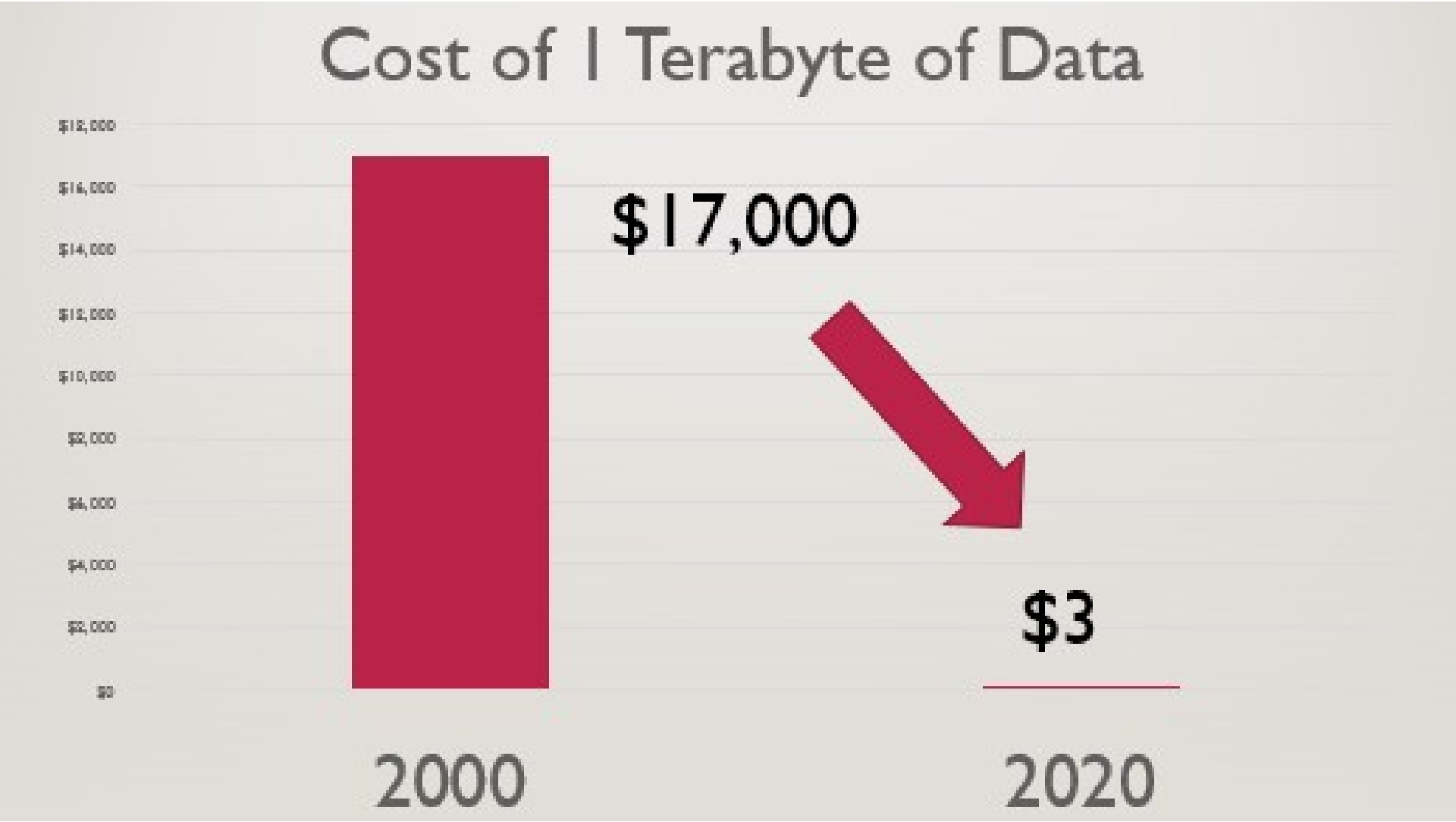
OFFICE OF THE
STATE

Remember



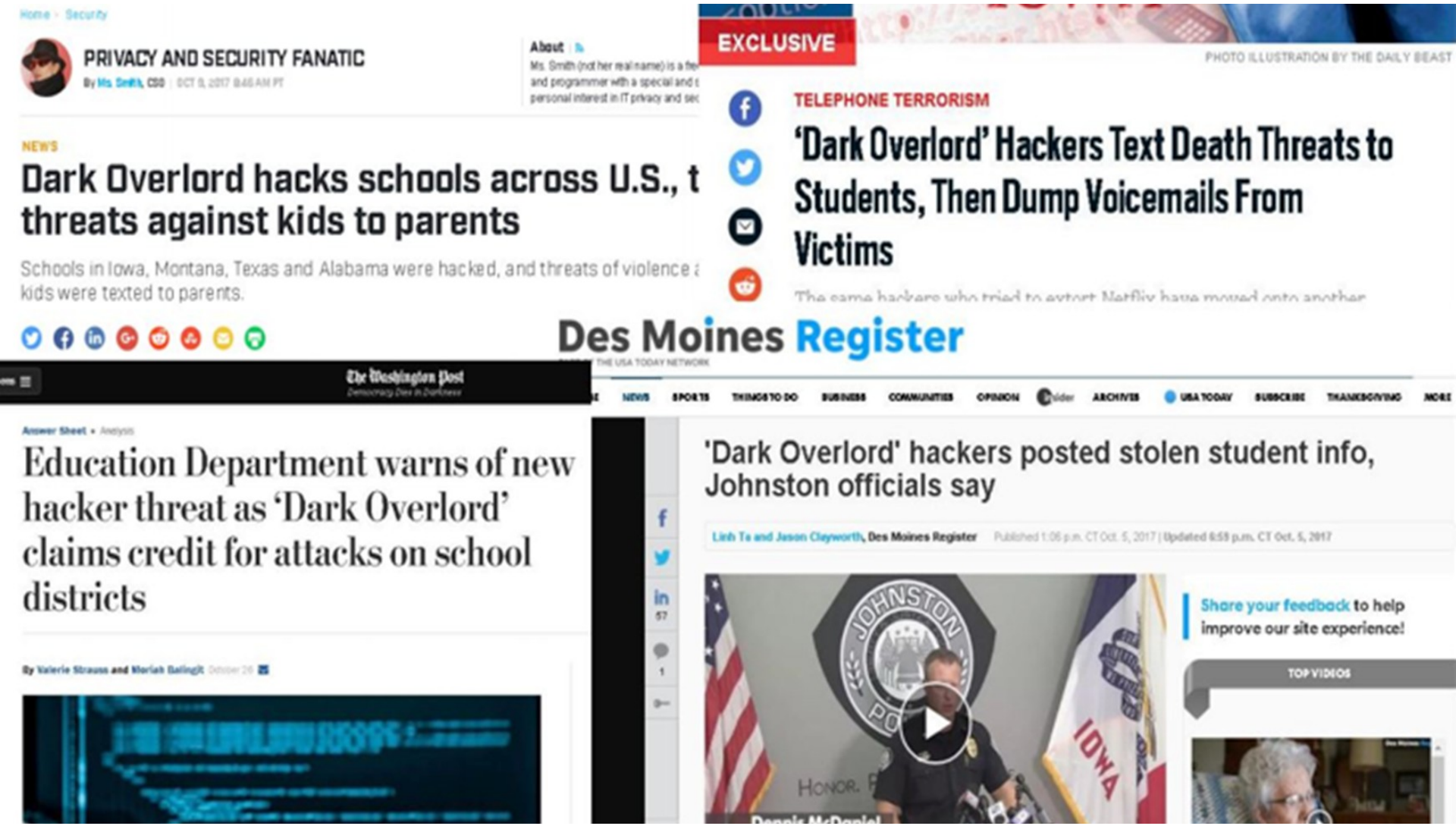
Why is the state government an attractive target?




Cost of 1 Terabyte of Data
$18,000
$16,000
$14,000
$12,000
$10,000
$8,000
$6,000
$4,000
$2,000
$0
$17,000
$3
2000
2020


THE RISKS
out of the
70 MILLION devices
lost or stolen each year
ONLY 7% recovered
15%
of employees have accessed sensitive data from non-work-sanctioned devices
54%
of organizations don't include employee-owned devices in their backup plans
65%
of companies cannot wipe devices remotely
76%
of companies do not encrypt mobile devices

OFFICE OF THE
STATE


Home › Security
PRIVACY AND SECURITY FANATIC
About
NEWS
Dark Overlord hacks schools across U.S., t
threats against kids to parents
Schools in Iowa, Montana, Texas and Alabama were hacked, and threats of violence a
kids were texted to parents.
EXCLUSIVE
PHOTO ILLUSTRATION BY THE DAILY BEAST
TELEPHONE TERRORISM
'Dark Overlord' Hackers Text Death Threats to Students, Then Dump Voicemails From Victims
Des Moines Register
THE USA TODAY NETWORK
The Washington Post
Democracy Dies in Darkness
NEWS
SPORTS
THINGS TO DO
BUSINESS
COMMUNITIES
OPINION
ARCHIVES
USA TODAY
SUBSCRIBE
THANKSGIVING
Answer Sheet • Analysis
Education Department warns of new hacker threat as 'Dark Overlord' claims credit for attacks on school districts
'Dark Overlord' hackers posted stolen student info, Johnston officials say
Linh Ta and Jason Clayworth, Des Moines Register
Share your feedback to help improve our site experience!
TOP VIDEOS
JOHNSTON
IOWA

OFFICE OF THE
STATE

OFFICE OF THE
STATE

TECH POLICY

The secret police: Cops built a shadowy surveillance machine in Minnesota after George Floyd's murder

An investigation by MIT Technology Review reveals a sprawling, technologically sophisticated system in Minnesota designed for closely monitoring protesters.

By Tate Ryan-Mosley & Sam Richards

March 3, 2022

2021 HB 243: Privacy Protection Amendments

Personal Privacy Oversight Commission (PPOC)	Two state privacy positions	Creates a reporting requirement
• Investigates complaints • Develops standards and best practices • Recommends legislation	• Government Operations Privacy Officer • State Privacy Officer	• Annually, on or before Oct 1, the commission shall report to the Judiciary Interim Committee

State Privacy Officer Responsibilities

1. Analyze and report on government privacy practices
2. Provide educational and training materials
3. Identify privacy practices that pose the greatest risk to individual privacy and prioritize those privacy practices for review
4. Respond to requests from individuals to review a designated government entity's privacy practice
5. Make privacy recommendations to the State Legislature

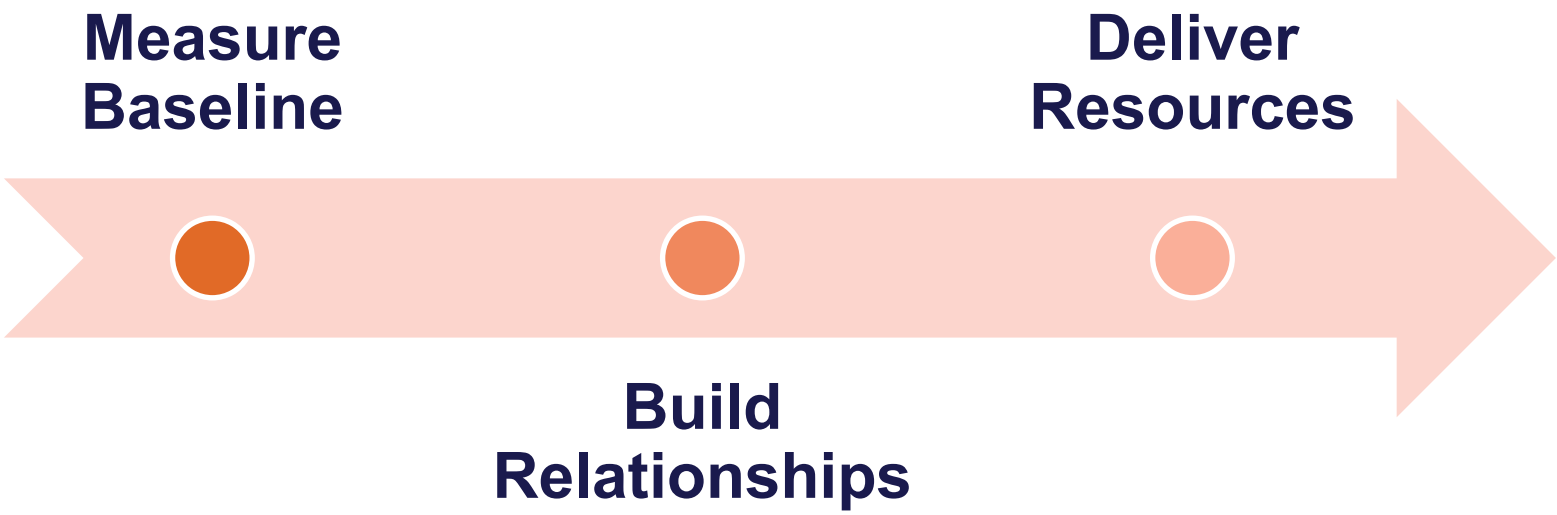
Scope

1,147 government entities:

- Local and Special Service District 391
- Local Education Agency 152
- City 146
- Town and townships 108
- Redevelopment /Project Area 89
- State of Utah (depts/comp, units) 67
- Interlocal 62
- Conservation District 38
- County 29
- Housing 19
- Institution of Higher Education 18
- Misc. 28

262,860 employees

My Plan: 2022

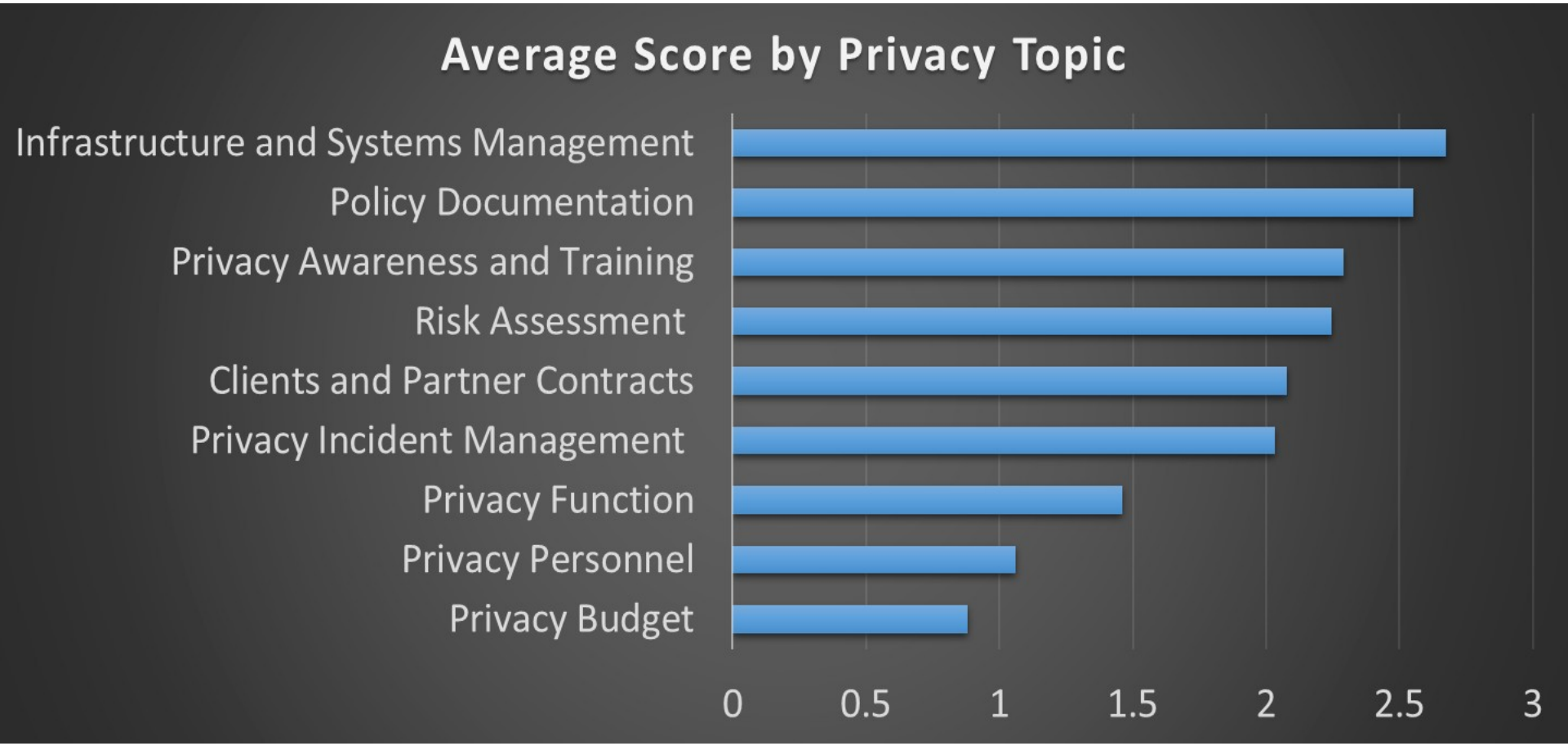


Privacy Maturity Survey

- All Local Education Agencies, 153
- All Counties, 29
- All other designated government entities with 50 or more employees, 168

*53% response rate

	Privacy Program Criteria								
Maturity Level	Contracts with Clients & Partners	Infrastructure & Systems Management	Policy Documentation	Privacy Awareness & Training	Privacy Budget	Privacy Function	Privacy Incident Management	Privacy Personnel	Risk Assessment
0	Contracts do not address privacy	Procurement of IT-related products & services do not address privacy	There are no documented privacy policies	Contents of privacy policies are never communicated with personnel	There is no budget specifically allocated to privacy purposes	There is no assigned privacy office or function	There is no way to respond to suspected incidents	No one person with a job description of a privacy officer	Project plans & acquisition of IT-related products do not address privacy
1	Confidentiality clauses are included incontracts, but compliance cannot be monitored	Project and IT managers occasionally address privacy in plans & system-development	Multiple, inconsistent policies, or policies that do not address all privacy principles	Some contents of privacy policies are communicated to some personnel	No specific budget, but privacy dollars are spent ad hoc as add-ons to other projects	One person assigned privacy responsibilites serves as the privacy function	Some personnel have knowledge and skills to respond to suspected incidents	At least one person is assigned privacy responsibility, but time commitment exceeds the person's availability	Project & IT managers occasionally address privacy in project plans & system development
2	Personnel review contracts for consistency with privacy policies	Policies require that IT products, services, and system development address privacy	Policies address all privacy principles, and are displayed on relevant websites.	Privacy policies are communicated annually to personnel who encounter PII	Specific budget sufficient to cover basic travel & subscriptions, and modest amount for special projects	Privacy function is identified in org charts, reflecting sustained commitment	Privacy incidents have been effectively resolved, but at most only high-level policy or procedures are documented	At least one person devoted exclusively to privacy, with sufficient staff assistance	Policies require acquisition of IT-related products & services address privacy
3	Standard contractual clauses are in place, and compliance can be monitored	Detailed checklists & procedrues are used to insure compliance with policies	Policies address all privacy principles, are publicly displayed, and details for implementation are included	Privacy policies are communicated annually to personnel who encounter PII and are provided role-based training	Specific budget that includes enough money to accomplish most privacy objectives	An executive committee member is formally assigned to be privacy champion, and an annual report is presented to board	Personnel have detailed roles and responsibilities, and detailed policies & procedures are maintained	Privacy staff have clearly defined job descriptions that require certification as CIPP, including at least one with a leadership title, and enough staff to meet most privacy objectives	Detailed checklists, procedures and assigned personnel to ensure all IT-related projectsare compliant with privacy policies
4	Standard privacy & secuity clauses and internal compliance are measured annually	Compliance with privacy policies of IT products and services are measured and routinely tested	Business operations, processes, etc. are reviewed annually, and are updated as needed	Personnel comprehension of, and compliance with privacy policies is measured annually	A "Balanced Privacy Scorecard" or other approach used to determine a budget sufficient to cover all objectives	The privacy function is placed in a particular dept to support its strategy, and has direct access to Executive Committee	Suspected incidents are routinely measured & tested for privacy compliance, improvements are made based on this	Privacy staff have clearly defined job descriptions that require certification as CIPP, a Chief Privacy Officer, and enough staff to meet all privacy objectives	Information-related products and services are routinely measured and tested for complance with privacy policies
5	Controls in place to prevent adoption of privacy & security commitments that cannot be kept	Controls in place to ensure IT products and services are compliant with policy and procedure	Policies & standards are compared annually to others, and have achieved "best practices" status	Policy compliance is compared annually to others, and have achieved "best practices" status	Privacy function funds are exceeded by privacy dollars spent elsewhere in the organization	The head of the privacy function has direct access to leadership and is a part of business strategy decision-making	All incidents are resolved within 30 days	Privacy objectives are in the job descriptions of all personnel who access PII	Controls in place to prevent new IT-related products and services from being deployed without being compliant with privacy policies


Average Score by Privacy Topic
Infrastructure and Systems Management
Policy Documentation
Privacy Awareness and Training
Risk Assessment
Clients and Partner Contracts
Privacy Incident Management
Privacy Function
Privacy Personnel
Privacy Budget
0
0.5
1
1.5
2
2.5
3

Top 10

8 Local Education Agencies (LEAs)

2 Behavioral Health Facilities

Bottom 10

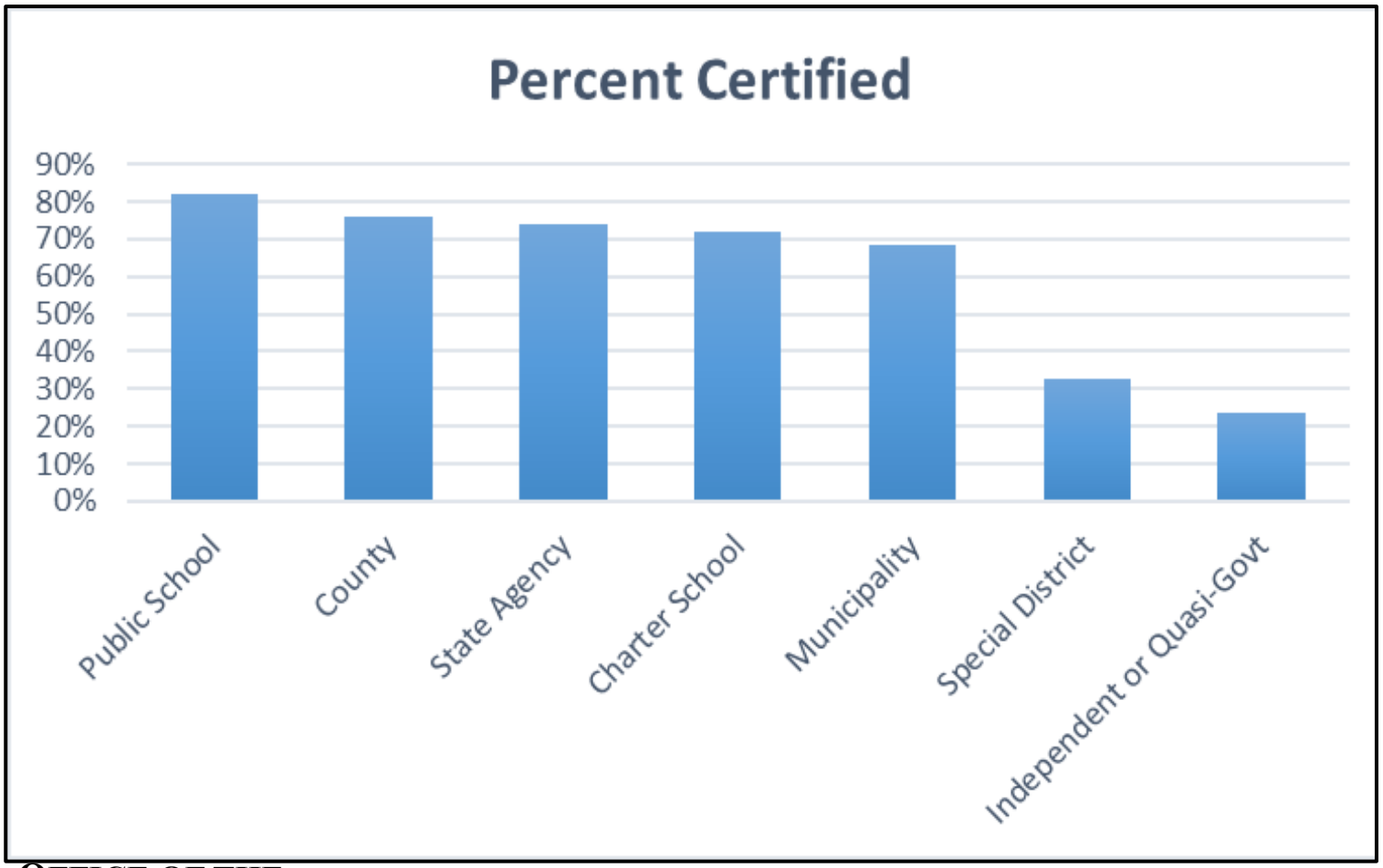
4 Counties

6 Cities

Government Records Access and Management Act (GRAMA)

- 63G-2-108 **Certification of records officer:** Annual certified Records Officer
- 62G-2-307 Duty to evaluate records and **make designations and classification**: Evaluate, designate, and report record's series that are used
- 63G-2-601 Rights of individuals on whom data is maintained–Classification statement–Notice to provider of information: Provide **purpose of data collection** to the state archivist, Collection notification

Current Records Officer Certification



Next Steps

Spring 2022

- Measure privacy maturing of medium and small government entities
- Develop City/Town and County Records Officer Certification Training

Summer 2022

- Train large designated government entities
- Hire additional privacy FTE

Fall 2022

- Legislative Report
- Train at Fall ULCT and UAC conferences

DON'T WAIT!

Certified Records Officer

Certified Information Privacy Manager (CIPM) Training (limited to 10)

- **June 21-22 Fall TBD**

Security+ training and certification (limited to 10)

- Summer and Fall TBD (5 sessions)

Remember